NEED TO KNOW
a national security newsletter

Volume 3, Number 2 January 2003

INEEL Establishes National SCADA Testbed

During an interview regarding National Security's critical infrastructure protection program, a reporter asked Associate Laboratory Director Laurin Dodd what could happen if a SCADA system were breached. Supervisory control and data acquisition or SCADA systems are used in almost every phase of energy production and distribution. As the name implies, SCADA systems control processes, often remotely. They are the communication and control systems used for planning, operation and maintenance of energy infrastructure grids.

According to industry experts, the "what ifs" of SCADA hacking are terrible and enormous, from shutting down whole power grids to the real-life example Dodd gave, maliciously releasing thousands of gallons of wastewater into the center of a metropolitan city.

But the INEEL isn't just talking about the risks to SCADA systems. The Laboratory is doing something about it. In collaboration with Sandia National Laboratories, the INEEL has established the National SCADA Testbed.

Modern gas circuit breakers looking like gigantic tinker toys dwarf an electrician standing by the control cabinet. INEEL power management recently completed upgrades to the site's high-voltage transmission distribution system. (above). INEEL SCADA Testbed project manager Steve Fernandez (right)

Steve Fernandez, INEEL's SCADA Testbed project manager, wrote the Joint Program Plan in intense sessions with Sandia counterpart Reynold Tamashiro. Fernandez and Tamashiro will serve as joint managers of the program and will oversee all tasks. The Department of Energy, Office of Energy Assurance, is funding the eight-year, $114 million program.

National Resource

"The National SCADA Testbed represents a new model within the DOE complex," said Fernandez. "The Testbed is one of the first and the National

See **TESTBED**, *page 2*

TESTBED *(continued from page 1)*

Infrastructure Simulation and Analysis Center is another, that are considered national resources. This means that not only DOE and other government agencies, but also industry can rely on these entities for expert information, science or recommendations in their respective areas."

According to Fernandez, the national resource concept goes beyond the traditional view of labs acting parochially and conducting individual tasks exclusively with their own researchers and engineers. The SCADA Program Plan encourages multi-organizational teaming between the core laboratories and industry experts for all of the separate tasks.

"Each of the core labs brings specific strengths to the SCADA Testbed and we'll take advantage of that," said Fernandez. "But the individual projects will be completed by a team of experts from not only both INEEL and Sandia, but also experts from other federal agencies, universities, or the energy industry, wherever the best folks are to get a specific task completed. That's how you not only get buy-in from all the stakeholders, but how you get considered a real national resource."

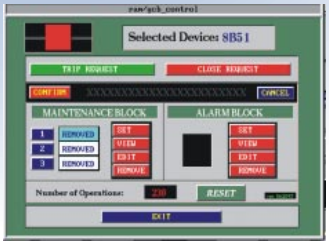
"We have assembled a team of experts to meet this challenge," said Sandia's Tamashiro. "Steve and I have built this program and our relationship based on trust and a shared common program vision, and our staff members have followed suit. We wanted to establish a long-term alliance between the two Labs by leveraging our strengths and jointly seeking areas of research."

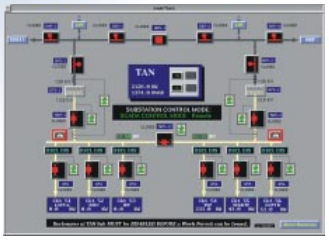
Testbed Defined

The vision for the Testbed, as defined in the program plan by INEEL and Sandia, encompasses far more than the vital hardware testing.

Fernandez explained that although it is called a Testbed, it is not concentrated on just hardware development. Staff will conduct vulnerability assessments of critical energy SCADA systems and will educate customers and stakeholders on the vulnerability risks. They will develop usable models to simulate system breakdowns and alternative courses of action. Members of the Testbed team will advise the government on standards and certification to increase the safety of existing and future energy systems. And they will be doing the science, and conducting research on the next-generation equipment, components and systems that can result in a self-healing infrastructure. One of the first tasks that the Testbed team undertakes will indicate the future path for research.

"The Testbed is made up of people, places and things," said Fernandez. "We have the people who can advise, experts who conduct the tests and the research. We have the places that simulate grid structure and we have things – the systems and





Power Management engineer Bob Henderson stands next to oil circuit breakers, whose controls were upgraded as part of the construction project. (above) The Test Area North acquired arc-resistant switchgear controlled by SCADA systems. (right and bottom)

components – for both testing and research."

Task 1.5

The reality of the National SCADA Testbed is evidenced by the magnitude of one of the first tasks. The team will establish recommended approaches for the electrical power industry to secure its SCADA systems.

The success of any set of recommendations is somewhat contingent on industry buy-in.

Power poles disappear in the distance on the INEEL's desert site.

If the industry doesn't feel that its needs or business restraints have been addressed, it will be reluctant to adopt the recommendations. Fernandez says that outreach is a requirement for success. The Testbed team recognizes this and will conduct a "virtual" workshop of leading industry representatives from the Electrical Power Research Institute, the Federal Energy Regulatory Commission and the Gas Technology Institute among others, to obtain input and review of the SCADA multi-level security document. Feedback will be incorporated into the final version before release industry-wide.

Above all else, this first major product will be grounded in reality and will clearly define what industry can do right now to safeguard SCADA systems. The document will also identify the path forward, establishing future direction for research and development.

Portal Concept

When asked how INEEL and Sandia will run the Testbed, Fernandez answers "seamlessly." The project plan established this philosophy with what it calls a "portal concept" for doing business. While the Testbed is managed through its Joint Program Office consisting of equal representation from INEEL and Sandia, it is called neither the INEEL nor Sandia program. It is *The* National SCADA Testbed and will be known nationally and internationally as such. The logo doesn't incorporate either laboratory name in its design and the Web site will link from each laboratory.

"I am pleased – no, impressed – by how quickly our two Labs have come together," said Tamashiro. "Our technical staff and management are committed to the challenge bestowed on us. We will be a national resource to both government and industry, and solve one of our nation's most recognized critical infrastructure vulnerabilities… SCADA."

This portal concept and the Testbed's role as a national resource even extend into Laboratory Directed Research and Development. Both laboratories are conducting LDRD projects on SCADA modeling and simulation – the INEEL on interactive 3D simulation using real data, and interdependency models, and Sandia on its power grid model, called Buzzard. Plans call for merging project results into one "super" simulation model that would then be moved to the National Infrastructure and Simulation Analysis Center for general industry use.

The National Security Division is already sponsoring other exciting LDRD projects in support of the Testbed including one to design self-healing infrastructures that has the healing elements built in, rather than patches put on … rather like getting a flu shot instead of taking aspirins and fever-reducers.

Today, the Joint Program Plan is eight years and $114 million. But Fernandez believes it will grow much larger, much sooner, with contributions from vendors, researchers and universities wishing to work and collaborate with the Testbed.

Steve Fernandez
sfernand@inel.gov

The "Eyes" Have It

INEEL engineer designs video camera for chem/bio response teams

National Guard Civil Support Teams have tough jobs. They are the ones summoned by firefighters to investigate incidents involving possible chemical, biological or radiological material. And like firemen or SWAT teams, they must wear safety gear. For protection against potentially deadly substances, CSTs don bubble-hooded, full-body Tyvex suits that, unfortunately, also limit visibility and mobility. Thus hampered, they may have to enter buildings or tunnels, in small groups, facing unknown dangers. Engineered Systems' Kevin Young has developed a nifty tool to help them "see" a little better – the Hazmat Cam.

Hazmat Cam is a lightweight, wireless video camera system. Housed in a tough, waterproof

See **HAZMAT CAM**, *page 4*

HAZMAT CAM *(continued from page 3)*

flashlight body, the camera system sends back real-time images to a computer or video monitor at the command post located outside the exclusion zone or contaminated area. Within the command post, the incident commander and any other experts can "see" exactly what the entry team sees. Involving the whole team in tactical analysis of a chem/bio or hazardous material incident increases responder safety and decreases assessment time.

Originally, Young conceived of a helmet-mounted camera for SWAT teams, but that design wouldn't work with the bubble hoods of hazmat crews. This hand-held device offers greater flexibility than a helmet-mounted camera with the added benefit of being completely waterproof. Thus, it can be easily decontaminated.

Hazmat Cam is a perfect example of the Engineered Systems' applied engineering and rapid prototyping strengths. In May 2001, Young rigged up a pilot version of the camera for a WMD conference. He scrounged parts and pieces, borrowed a transmitter and transceiver from an INEEL robotics group, and came up with a credible demonstration version. South Carolina's CST members were enthralled with the concept and traveled through the conference aisles, camera in hand. Less than 16 weeks later, Young demonstrated the first-generation Hazmat Cam in South Carolina.

"I've listened to the different chem/bio teams during training exercises and at meetings and conferences," says Young. "The most important requirement for a camera is clean, clear, reliable video."

True-diversity Receiver

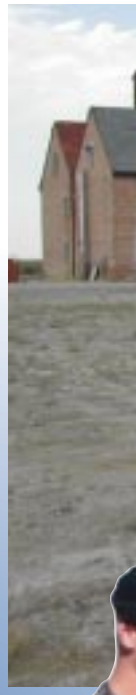
Integral to Hazmat Cam's fidelity is its triple-antenna, true-diversity receiver. Traditional wireless video uses one antenna and a single receiver. The problem with this configuration is that signals multi-path – they bounce off other structures, buildings, file cabinets, even people – on their way to the receiver. This causes interference and seriously degrades the video images. Since users of any hand-held wireless camera are constantly moving, the problem is compounded. The Hazmat Cam receiver seeks the strongest signal from each of the three antennas and locks in this signal. It completes this scan over 1,000 times per second, much faster than a human viewer would notice. This triple diversity receiver results in a clearer, more reliable image even under less than perfect conditions such as within metal buildings, or concrete tunnels.

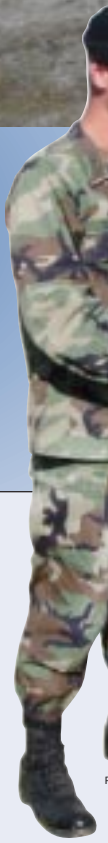
Young lifted the idea of using the triple antenna configuration straight from his experience as a jazz musician.

"I took the idea from my music," says Young, who plays the saxophone. "Based on my experience with wireless microphones, I knew a diversity receiver was the way to go. Performers move around the


PD03-0027-02

National Guard Civil Support Team members gear up for an exercise. Hazmat Cam has been used in CST field exercises throughout the country.






PN03-0003-02-05

State of the Division

Laurin Dodd,
Associate Laboratory Director, National Security

2002 was another very good year for the National Security Division.

I congratulate all of the staff for their hard work and innovation. Your achievements continue to enhance INEEL's reputation as a national laboratory that performs quality work within budget and schedule. And I thank our clients for providing us the opportunity to work with them in addressing problems important to our nation's security.

Preliminary ratings by DOE for INEEL's overall performance in 2002 are in. Once again, the Laboratory has achieved an overall rating of over 90 percent. The National Security Division made significant contributions to this high rating.

Most important to our future is the significant progress we have made toward a major goal that we set just less than a year ago. Following the terrorist attacks in New York and Washington, it became clear that our nation's infrastructures faced levels of risk that are unacceptable. There is a national need to better understand and to mitigate the risks, and ultimately, to design 'smart infrastructures' that are inherently less vulnerable to attacks. It also became clear that the engineering discipline – and many of the INEEL's 'critical infrastructures' – made the Laboratory an ideal place to support both government and industry research and development for better protection of infrastructures critical to the operation of our country.

During the last 12 months, we have made significant headway in establishing the INEEL's comprehensive Critical Infrastructure Assurance Program. Here are a few highlights:


PD03-0027-01

CST Sampling unit prepares to enter a training site in Dugway, Utah, after the reconnaissance team had done their job. The recon team used Hazmat Cam to send real-time images that provided valuable information on sampling sites and equipment needed to continue the operation.


PD03-0027-03

stage. All of the really good wireless audio technology uses diversity receivers."

The 900-MHz transmission can still be subject to interference from such devices as wireless phones and pagers, but that can usually be overcome by switching channels. A more difficult problem for any wireless system is the really large transmitters, such as those at airports. These transmitters create harmonics so huge they overpower most transmitter systems.

"There is no RF camera system that will work in every environment," says Young, "but we have developed a system that works well in most." Hazmat Cam has been rigorously tested by CSTs and firefighters during field training exercises conducted throughout the country. The first systems were purchased in December.

Extension Link

Hazmat Cam has other features that distinguish it from existing systems. Extension Link is a separate transmitter-and-receiver system that increases the operating range of the Hazmat Cam by two to three miles. It operates at higher power and has field-selectable channels to avoid interference at the longer distances.

The current version of Hazmat Cam includes optional encryption so that, according to Young, CNN can't pick up the transmission and broadcast it on the evening news. This doesn't mean, however, that the transmission can't be shared among cooperating agencies. Agencies on the scene with properly configured Hazmat Cam receivers can all receive the same video transmission.

The Engineered Systems organization, led by department manager Ken Watts, has supported the design, development and marketing phases of this project. Colleagues Yvette Leppert and Stacey Barker have immersed themselves in the camera design and capabilities, fielding questions and conducting demonstrations. And Young credits the technicians who build Hazmat Cam – Brent Smith, Bob Denkers and Paul Mottishaw – with the system's simplicity and robustness.

"What makes Hazmat Cam so good," summarizes Young, "is that it uses off-the-shelf components integrated in an innovative way."

Kevin Young
youngkl@inel.gov

- A methodical evaluation of INEEL capabilities was made, resulting in a Web-based catalog supported by an asset and facility directory that allows a thorough analysis of test range locations, scenarios and opportunities, and also offers professional informational materials.
- A detailed management plan was developed that will guide Test Range growth and maturity.
- U.S. Sen. Larry Craig announced in July his intentions to support the Laboratory as a Critical Infrastructure Test Range. "The new Department of Homeland Security must have access to the absolute best that the DOE National Laboratories have to offer," Craig said. "Specifically, the INEEL is uniquely suited to serve as a Critical Infrastructure Testing Station. I will be working – both legislatively and with the Administration – to have INEEL's capabilities acknowledged and available to the new Department." Craig developed legislation to fund the Test Range.
- In partnership with Sandia National Laboratories, the INEEL established the National Supervisory Control and Data Acquisition (SCADA) Testbed. We co-authored the eight-year, $114 million Project Management Plan and delivered it to the DOE Office of Energy Assurance at year-end.
- Construction of three cell towers for the Wireless Testbed is under way and completion is anticipated in late January. This is funded through a Cooperative Research and Development Agreement (CRADA) with Bechtel Telecommunications and a Corporate Funded Research and Development project (CFRD) with Bechtel National.

We completed construction of an 820-square-foot, class 1000 cleanroom in April. This project was funded by the U.S. Air Force. The cleanroom enhances our ability to provide ultratrace environmental analysis.

Another highlight for the year is captured in the article on explosives detections. Real progress has been made in exploiting INEEL-developed technologies for detecting explosives from a distance.

Finally, I would like to once again congratulate Jack Way and his staff on their exceptional effort in conducting the only Counterintelligence Program within the DOE complex to earn an overall 'excellent' rating with 'no findings.'

Better Than Dogs

INEEL Technologies "Sniff Out" Smuggled Explosives

With a one-upmanship on nature, National Security scientists are developing a technology that will eventually detect explosives hidden in a vehicle faster and from a greater and safer distance than is possible with bomb-sniffing dogs. Using neutron technology, the researchers can already detect the presence of an explosive surrogate sealed within a car trunk at a stand-off distance of three meters in a mere 400 seconds.

Long the standard of military and law enforcement, bomb dogs can work a vehicle, sniffing tires, doors, trunks and hoods in about five minutes. That time does not include removing the vehicle from a traffic line or staging it for inspection. And for effective detection, the dogs must have access to the compartments in a suspect car, van or truck that might conceal the explosives. A customer, looking for increased security measures for vehicles entering military bases, asked INEEL researchers to try and develop a technology that improves on the labor-intensive practice of using canines.

"Before we considered any solution, we investigated every possible technology out there now," said Mike Occhionero, program manager for the Remote Standoff Explosive Detection project. "After a comprehensive evaluation of potential stand-off explosive technologies by our whole team of engineers and explosives experts, we drew the conclusion that only an active interrogation system would work."

Two Solutions

INEEL researchers actually came up with two potential solutions and demonstrated their capabilities to military representatives this past summer. Both systems use existing INEEL-developed neutron activation technologies, optimized for explosives detection. One solution is based on the Portable Isotopic Neutron Spectroscopy (PINS) system, an R&D 100 award-winning technology traditionally employed by the military to identify the contents of suspect chemical weapons. The other solution uses an accelerator about the size and maneuverability of automobile diagnostic computers. Both target the suspect vehicle or container with low levels of neutrons, and then analyze the characteristic gamma-ray response of specific chemical elements. This first test was simply intended to demonstrate the technologies' ability to detect the explosive at all, and then, hopefully, at up to one meter.

James Jones describes the accelerator-based explosives detection technology to representatives from the Department of Defense Physical Security Equipment Action Group. (top) Gus Caffrey, holding a next-generation neutron detector, demonstrated PINS' ability to detect explosives (below left). The electron accelerator used in the research program (below right)

PN02-0616-01-22

PN02-0616-01-27

PN02-0616-01-30

Both PINS and the accelerator conclusively identified the surrogate explosive, but after some system design changes based on numerical modeling predictions, the INEEL scientists demonstrated the accelerator's ability to detect the material at three times the original distance.

"We weren't actually expecting to be able to detect it from that far that soon," said Occhionero. "But now that we have, our next goals include doing it even faster, lowering the detection time."

Additional demonstrations were conducted in October before representatives of the Department of Defense Physical Security Equipment Action Group. PSEAG members evaluate research programs and technologies supporting military security programs.

The demonstrations mimicked one possible implementation scenario, in which the inspection system would be placed underground. After the two researchers conducted the

The INEEL-developed technologies detected the surrogate explosives concealed within this car trunk.

PN02-0616-01-30

separate tests – Gus Caffrey first ran PINS, then James Jones ran the accelerator test – they fielded questions from the PSEAG members.

Many of the questions centered on shielding. Terrorists could attempt to shield the explosives with everything from lead to polyethylene. Caffrey responded.

"Massive amounts of lead would be needed to shield the bottom of a vehicle – as much as four inches of lead," explained Caffrey. "PINS would see the lead gamma rays. Materials used in shielding would reveal themselves in the gamma signatures of any neutron activation system."

PN02-0616-01-08

Research Continues

Research continues on increasing the distance and reducing the time of detection, and also on ensuring the safety of operators and civilians. The precedent for successfully using these types of systems exists in everyday applications from dental X-rays to mining, where small neutron generators are lowered into wells. The PINS system is already safely and successfully used worldwide. As in all scientific or industrial processes, safety is ensured through the engineered design of the system and the process for using it.

Occhionero and team members are evaluating concepts for integrating the technologies into military base security.

"We are looking at a lot of ideas, including placing the system underground," said Occhionero. "Not only would that make it easy to inspect vehicles, the placement would offer excellent shielding."

"We believe the system could be used many places besides military bases, such as in federal building parking garages and even U.S. embassy driveways," said Occhionero. "We proved we could do it, now we want to optimize the design and get it out into the field."

Explosive detection research is one part of the INEEL's overall critical infrastructure protection program, in which technologies, systems and policies that protect the nation's core systems – such as energy, communications and transportation – are developed, tested and validated under real-world conditions. Other technologies being developed include a system to protect our nation's ports by detecting smuggled nuclear materials in huge cargo containers, and one that preserves our reliance on oil and gas pipelines by pinpointing damage to pipelines and transmitting that data to a central location. The critical infrastructure protection program encompasses vast physical test ranges for critical infrastructure including next generation wireless communications and SCADA (supervisory control and data acquisition) systems.

Michael Occhionero
occhmp@inel.gov

Portable Isotopic Neutron Spectroscopy System (PINS) shrinks in size, not stature

INEEL Cooperative Research and Development Agreement partner, Ortec, delivered the first four commercial miniPINS systems to the U.S. Army. MiniPins was developed to reduce set-up time and shipping costs for its many customers who send the systems and field technicians around the country and around the world. A comparison of the two systems reveals the differences.

PD03-0027-04

	miniPins	standard PINS
Weight (detector and stand)	46 lbs.	96 lbs.
Electrical power usage	5 watts	15 watts
Battery life	8 hours	8 hours
Shipping containers	3 (192 lbs. total) 14.6 cu. ft.	7 (409 lbs. total) 37 cu. ft.

Why Spy?

Contributed by: Gene Johannes

"The creditors were hounding me! We weren't supporting or treating them the way we should have. They were going to give my wife photographs of my girlfriend and me; it would have ruined my marriage. My boss promoted the 'yes' people instead of me."

The top five primary motives for spying, based upon 150 cases* evaluated, were:

- Money – 56%
- Divided Loyalties – 17%
- Disgruntlement – 13%
- Ingratiation – 10%
- Coercion – 3%

Spying does happen and the threat is real. Since the end of the Cold War, our former "adversaries" and some "friends" have shifted the priorities of their intelligence collection assets from military/defense information to economic/emerging technologies. This does not mean that military/defense information is not targeted, just that economic/emerging technological information has become the primary target for collection. With world markets and economies becoming more interdependent, the acquisition of technological and economic information has become vital to compete in the global economy. This competition has contributed greatly to the incentive, motivation and opportunities for people to illegally collect and transfer technological or economic information.

What Can I Do?

Be alert. If it "just doesn't look right" (JDLR), report it. Some indicators of possible inappropriate conduct are

- Lifestyle inconsistent with known income.
- Marked changes in character, attitude, emotional stability, work habits, etc.
- Criminal or immoral conduct.
- Excessive use of intoxicants or use of dangerous drugs.
- Travel to distant locations or countries inconsistent with one's interest or means.
- Repeated overtime work or visits to work areas after hours for no logical reason.
- Undue curiosity about matters not within the scope of the individual's job.

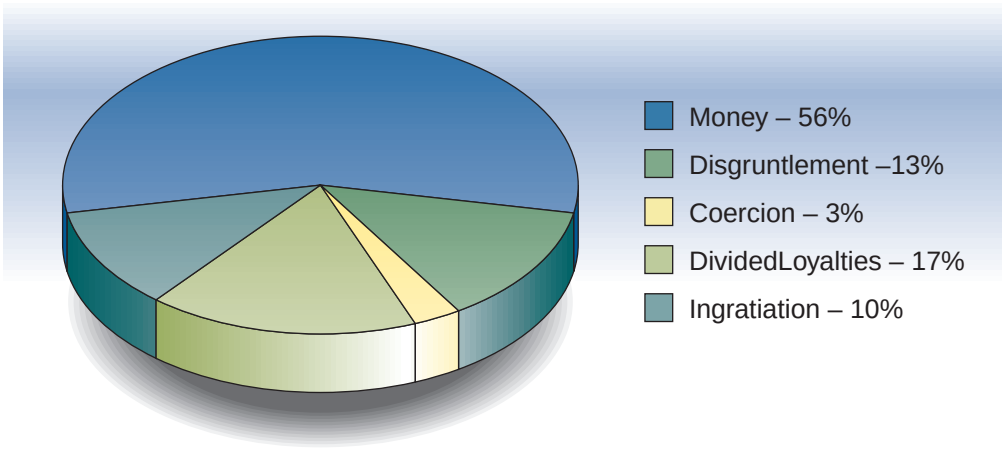
This list is not all-inclusive, nor does it mean that if an individual displays one of the above indicators, he/she is a spy. These are merely indicators. Most individuals convicted of spying have displayed more than one indicator. If an individual displays indicators that just don't look right and cause you to think something is wrong, report it. Counterintelligence will discretely investigate the information to confirm or refute any acts relevant to the illegal release/transmission of sensitive/classified information.

Counterintelligence staff can be reached at:

Telephone:
526-2223/4023/3661

e-mail:
xjw@inel.gov
johace@inel.gov
crandacb@inel.gov

Top Five Primary Motives for Spying*



* Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by American Citizens 1947-2001*, pp39, Technical Report 02-5, Defense Personnel Security Research Center, Monterey, CA, July 2002.

NEED TO KNOW *is a publication of the National Security Division of the Idaho National Engineering and Environmental Laboratory. The INEEL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's missions in environment, energy, science and national security. The INEEL is operated for the DOE by Bechtel BWXT Idaho, LLC. Requests for additional copies, story ideas or questions should be directed to the editor at (208) 526-1058, kzc@inel.gov. This is printed on recycled paper.*

Editor ..... Kathy Gatens
Graphic artist .... David Combs
Photographers .. Mike Crane, Chris Morgan, Ron Paarmann
Copy editing ..... Rick Bolton

Visit our national security website at:
www.inel.gov/nationalsecurity